Press release

Jyske Bank A/S
Vestergade 8-16
DK-8600 Silkeborg
Tel.: +45 89 89 89 89
www.jyskebank.dk
Email: jyskebank@jyskebank.dk
Business reg. No. (CVR-nr.) 17616617

6 July 2017

The Danish Financial Supervisory Authority's report on IT inspection

In connection with the report, Managing Director Leif Larsen states:

"We have taken note of the FSA's conclusions following its inspection in 2016, and the bank has already addressed several of these.

It is reassuring that the inspection did not establish any serious shortcomings in Jyske Bank's actual IT security, as the critical remarks of the FSA primarily point out the need for increasing formalisation and control in connection with the bank's identification, assessment and reporting of IT security-related risks. We acknowledge that correct handling of the issues pointed out, including professionalization of the cooperation with outsourcing partners, will be a contributing factor ensuring that Jyske Bank always maintains a high IT security level, which is the bank's utmost priority".

Yours faithfully

Jyske Bank

Contact person: Managing Director Leif F. Larsen, tel.: +45 89 89 20 05

FINANSTILSYNET

FINANSTILSYNET
(Danish Financial
Supervisory Authority)

3 July 2017

Report on IT inspection at Jyske Bank A/S

1. Introduction

In 2016, the FSA conducted an inspection of the IT area at Jyske Bank A/S.

The FSA reviewed selected parts of the IT area, including general IT security management, IT strategy, organisation, disaster recovery/ contingency plans, security policies and guidelines. Moreover, the FSA reviewed Jyske Bank's procedures for the control of access to systems and data, change management, systems audit, control of outsourced IT functions and also requirements and procedures relating to control and reporting.

2. Summary and risk assessment

It is the assessment of the FSA that Jyske Bank has not established sufficient management and reporting in the area of IT security. This has resulted in the risk that the executive board and the supervisory board will not be informed to a sufficient degree of the actual IT risk picture. The FSA also assesses that Jyske Bank is not fully compliant with the statutory requirements in the IT area, including the bank's outsourcing of material IT activities.

The FSA has ordered Jyske Bank to strengthen its IT security management and management reporting as well as to improve the on-going control and follow-up on the actual IT security implementation both at the bank and the IT suppliers. Moreover, the management's requirements and expectations of IT-security work, etc. must to a higher degree be specified and documented.

Moreover, the FSA has ordered Jyske Bank to establish a sufficient method for IT risk management, covering both the bank and the performance of tasks at IT suppliers to whom such tasks are outsourced.

Among other things, improved documentation must be established of the correlation between IT risks and preventive controls and security measures that form the basis of the bank's IT security management. Moreover, Jyske Bank must ensure that sufficient requirements of roles and allocation of responsibility in connection with the IT security work are established.

Jyske Bank has also been ordered to ensure that the bank's internal business procedures and requirements according to the Executive Order on outsourcing significant areas of activity will be complied with to a sufficient degree.

In addition, the FSA has ordered Jyske Bank to improve its requirements of change management, including sufficient follow-up and control of changes to its production systems, separation of duties as well as access to confidential data.

Jyske Bank has been ordered to ensure that sufficient assessments of risks and consequences are prepared as a basis of disaster recovery/contingency objectives and disaster recovery/contingency plans. Moreover, Jyske Bank must improve requirements and business procedures for the coordination of disaster recovery/contingency measures at the bank and at material outsourcing suppliers. Business procedures and requirements of tests of disaster recovery/contingency plans must be strengthened, and moreover it must be ensured that disaster recovery/contingency plans and relevant test scenarios are tested to a sufficient degree.

Also, the FSA has ordered Jyske Bank to improve the management of access and rights to systems and data. At the same time, it must be ensured that adequate requirements for IT security logging are defined on the basis of risk assessment.